CERT: completes the IT Security and Risk Management Cycle allowing events to be proactively managed, responses to be dynamic and impacts and risks accurately measured.

CERT

A Computer Emergency Response Team (CERT) or Security Incident Response Team (SIRT) is a unit responsible for investigating and reporting on suspected security incidents. CERT minimizes the impact of security incidents, promotes compliance with IT usage policies, enables the tracking and understanding of incidents, provides advisories to IT security and IT user base about threats, quantifies loss and risk from security incidents and detects and deters advanced threats.

CERT capabilities include:

- Root cause analysis, to understand where security failures occurred, so that they can be corrected
- Generate alerts and advisories to users of IT systems
- Notify SOC staff of new threats to aid detection efforts
- Notify IT staff of potential security vulnerabilities
- Provide metrics to assess loss and risk from incidents
- Report critical findings or failures to management

Forward Defense CERT Training

Training will be required in a number of disciplines for all team members

- Network Fundamentals
- Incident Handling
- Log Analysis
- Network Monitoring
- Malware Analysis
- Forensic Collection and Analysis
- Penetration Testing

CERT: completes the IT Security and Risk Management Cycle allowing events to be proactively managed, responses to be dynamic and impacts and risks accurately measured.

Cert Staff Requirements

- Extremely knowledgeable in a variety of areas:
  - Networking
  - Log analysis
  - Malware analysis
  - Digital forensics
  - Penetration testing
- Must have an investigative mindset and be very interested in technology
- Must be extremely trustworthy with proper security clearances

Tools

A variety of tools will be needed to support a CERT

- Centralized Logging
- Automated Detection
- Intelligence Feed System
- Incident Tracking System
- Network Monitoring
- Enterprise Forensic System

Policies and Procedures

- Must be repeatable, remain nimble so as to enable rapid response, be forensically sound, maintain defensible evidence, and be in line with relevant standards
- Should adopt relevant requirements from ISO 17025, ISO 27035 and organizational policies and procedures
- Should define clear authorizations and reporting lines to ensure correct distribution of sensitive material

Summary

- Today's attackers are investing in stealing your data
- You must invest in protecting it
- Modern IT Security must be Proactive not merely Preventive
- Implementing a CERT to investigate anomalies on your network is the most effective way to address the current and future threats
- Feedback from a CERT provides quantifiable data to identify and assess risks to your organization, allowing informed business decisions

Contact Us

Each of our solutions is as unique as our customers. Please contact us to discuss the best way to meet all of your digital forensics requirements

www.forwarddefense.com
info@forwarddefense.com

Forward Defense Equipment and Services

51st Floor, Addax Tower City of Lights
Al Reem Island PO Box 47019 Abu Dhabi, UAE

+971 2 627 8921